Science and Technology Law Review

Volume 18 | Number 1 Article 2

2015

In Search of the Golden Mean: Examining the Impact of the President's Proposed Changes to the CFAA on Combatting Insider Misuse

Shawn E. Tuma

In Search of the Golden Mean: Examining the Impact of the President's Proposed Changes to the CFAA on Combatting Insider Misuse

*Shawn E. Tuma**

> That moral virtue is a mean, then, and in what sense it is so, and that it is a mean between two vices, the one involving excess, the other deficiency, and that it is such because its character is to aim at what is intermediate in passions and in actions, has been sufficiently stated.
>
> * * *
>
> So much, then, is plain, that the intermediate state is in all things to be praised, but that we must incline sometimes towards the excess, sometimes towards the deficiency; for so shall we most easily hit the mean and what is right.[1]

I. Introduction

Aristotle's description of the Golden Mean eloquently describes the struggles the United States Legislature experienced when attempting to find the right balance for the Computer Fraud and Abuse Act (CFAA). This struggle is especially prevalent when one applies the CFAA's regulations to cases involving privileged users. The struggle continues.

In his 2015 State of the Union address, President Barack Obama made the case for amending the CFAA's "exceeding authorized access" definition. According to the White House, the proposed amendment "modernizes the [CFAA] by . . . making clear that it can be used to prosecute insiders who abuse their ability to access information to use it for their own purposes."[2] While the President deserves to be commended for focusing the nation's attention on cybersecurity risks as a pervasive threat to our society, whether the proposed legislation would accomplish the stated objective is another issue.

---

* Partner, Scheef & Stone, L.L.P., Frisco, Texas. Website: www.solidcounsel.com. B.A., Northwestern State University, *with honors*; J.D., Regent University School of Law, *magna cum laude*. Mr. Tuma would like to thank his wife, Rachel, and five children, Katherine, Seth, Andrew, Christopher, and Clara for their loving support and understanding during the preparation of this article.

1. Aristotle, Nicomachean Ethics, Book II. Ch. 9.

2. *SECURING CYBERSPACE – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*, The White House (Jan. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat; *see Updated Administration Proposal: Law Enforcement Provisions*, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools-section-by-section.pdf [hereinafter *CFAA Amendment*].

The CFAA is a criminal statute that was enacted in 1986.[3] In 1994, an amendment to the statute added a provision that allows a complainant to bring a private civil cause of action for many violations of the Act.[4] Generally, the CFAA prohibits the misuse of computers by intentionally or knowingly accessing a computer "without authorization" or by "exceed[ing] authorized access."[5] In theory, the statute indicates that the "without authorization" prong *should* apply to users who do not have any access privileges. These individuals are referred to as "outsiders." The "exceeds authorized access" prong applies to individuals who have limited access privileges. These users are referred to as "insiders" or "privileged users." In practice, however, there is significant confusion between the two concepts, and in some cases these prongs are used interchangeably. The interchangeability of the two concepts will be discussed in more detail below. At this point it is sufficient to simply recognize the confusion between the two prongs of the CFAA.

This article examines two structural changes to the statutory language of the CFAA that the President recommends in the CFAA Amendment. First, it examines the negation of the civil cause of action under the CFAA, which the author of this article presumes to be inadvertent. This negation would occur if the factors set forth in subsection (c)(4)(A)(i)[6] were removed, as recommended by the CFAA Amendment. Second, the article examines the amended definition of "exceeding authorized access," and analyzes how the change in language will impact the overall objective of combatting insider misuse of computers and data.

Ultimately, this article concludes that, while the proposed amendment's language may help resolve one aspect of the confusion, it would only create more confusion elsewhere. Additionally, the proposed amendment would still fail to achieve its stated objective of achieving a better balance. The CFAA Amendment attempts to find the Golden Mean, but instead of attaining the desired balance, it continues to shift between excess and deficiency.

A. The CFAA Amendment Proposes—Hopefully Inadvertently—the Elimination of the Civil Cause of Action

The CFAA Amendment, if enacted as written, would eliminate the civil cause of action under the CFAA. It appears this change was inadvertent because language that supports the civil cause of action still remains in the amendment. What is intriguing is how, or why, the drafters could have inadvertently negated such an essential element to the statute.

3. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213 (codified at 18 U.S.C. § 1030 (2008)).

4. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R. FED. 101 (2001).

5. 18 U.S.C. § 1030(a)(1) (2008).

6. 18 U.S.C. § 1030(c)(4)(A)(i) (2008).

While the CFAA is primarily a criminal statute, it also provides for a civil cause of action and economic damages.[7] The procedure for invoking the civil remedy is complex, and therefore, has proven to be a fruitful area for litigation.[8] Navigating it correctly has proven to be as much of a challenge for judges[9] as it has been for lawyers.[10] Perhaps it was equally challenging for the White House.

The CFAA provides two requirements for a private right of action.[11] First, section 1030(g) provides that a civil cause of action is available to "[a]ny person who suffers damage or loss [from a violation of the CFAA]"[12] Second, civil remedies are restricted to claims arising out of conduct involving one of the five factors in subsection (c)(4)(A)(i).[13] These factors include:

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related

7. Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC, 774 F.3d 1065, 1072 (6th Cir. 2014) (citing 18 U.S.C. § 1030(g), (c)(4)(A)(i)(I)). ("The CFAA is primarily a criminal statute, but it also provides for a civil right of action and economic damages in certain circumstances, such as when a violator causes a 'loss' of at least $5,000 in value to one or more persons during any one-year period.").

8. Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?" A Primer on the Computer Fraud & Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 182 (2011) (noting that the terms used most frequently in CFAA's civil litigation are access and damage, and explaining that loss is explicitly required to plaintiffs who file under (c)(4)(A)(i)(I)).

9. *See* Shawn Tuma, *Yes, Texas is a Good State for Plaintiffs to Bring a CFAA Claim*, BUSINESS CYBER RISK LAW BLOG (Feb. 14, 2015), http://shawnetuma.com/2014/03/08/yes-texas-is-a-good-state-for-plaintiffs-with-a-cfaa-claim/ (critiquing a recent ruling on a motion to dismiss where the court failed to distinguish between losses and damages under the CFAA.); *see also* Shawn Tuma, *Loss and Damage Are Not Interchangeable Under CFAA–District Court Blows Right Past CFAA's "Loss" Requirement in* Sysco Corp. v. Katz, BUSINESS CYBER RISK LAW BLOG (Feb. 14, 2015), http://shawnetuma.com/2013/10/13/loss-and-damage-are-not-interchangeable-under-cfaa-district-court-blows-right-past-cfaas-loss-requirement-in-sysco-corp-v-katz/ (critiquing the court's interchangeable treatment of the loss and damage requirements by referencing the statutory language of section 1030(g) "[a] civil action . . . may be brought only if" as clearly stating otherwise).

10. Tuma, *Yes, Texas is a Good State for Plaintiffs*, *supra* note 9, at 184 n.352 (noting that "many of the CFAA cases that are dismissed for failure to adequately state a claim are dismissed because the plaintiff has not met this threshold pleading requirement").

11. 18 U.S.C. § 1030(g) (2008).

12. *Id.*

13. *Id.*

> course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; [or] (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security . . . .[14]

A plaintiff must plead the damage or loss precisely in order to bring a civil CFAA claim. This is because pleading loss or damage, through the factors present in subsection (c)(4)(A)(i), is an absolute requirement.[15] Of the five factors, the overwhelmingly dominant factor used in civil cases[16] is (I): "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[17] For example, the plaintiff must plead that, during any one year period, she sustained a loss of at least $5,000 because of a CFAA violation.[18] Each of the statutory requirements—damage or loss and a violation of one of the subsection (c)(4)(A)(i) factors—must be satisfied before the CFAA vests the court with jurisdiction.[19] Thus, the CFAA civil remedy is predicated on the existence of conduct violating one of the first five factors of subsection (c)(4)(A)(i).

Yet, the CFAA Amendment completely eliminates subsection (c)(4)(A)(i) without replacing it or removing the mandatory language for a civil cause of action: "[a] civil action for a violation of this section may be brought *only if* the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."[20] With subsection (c)(4)(A)(i) removed from the CFAA amendment, were it to pass, it would no longer be possible to properly plead a civil cause of action under the CFAA.

It would be a terrible mistake to remove the civil cause of action from the CFAA, whether intentionally or inadvertently. If this private cause of action is removed, the CFAA's enforcement is exclusively left to federal en-

14. 18 U.S.C. § 1030(c)(4)(A)(i)(I)–(V) (2008).

15. Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC, 774 F.3d 1065, 1072 (6th Cir. 2014).

16. Tuma, *Yes, Texas is a Good State for Plaintiffs*, *supra* note 9, at 183.

17. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (2008).

18. Grant Mfg. & Alloying, Inc. v. McIlvain, 499 F. App'x. 157, 159 (3d Cir. 2012); A.V. *ex rel.* Vanderhyne v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009).

19. *See* Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010).

20. 18 U.S.C. § 1030(g) (emphasis added).

tities. Unfortunately, the federal law enforcement and prosecutors that pursue the vast majority of the criminal CFAA cases lack the resources to consistently pursue all but the most substantial violations.[21] Because of this, many of the CFAA violations would never be pursued if not for private parties' ability to pursue their own civil cause of action against the violating user. This is especially true in many of the cases involving users that have privileges to use the computers (*i.e.*, "privileged users" or "insiders") but abuse those privileges to misuse either the computers or the data accessible through them. Additionally, many insider cases are less likely to warrant criminal prosecution because they do not involve financial losses in the millions of dollars, a threat to public health and safety, national security, or a threat to the United States' critical infrastructure.[22]

For these reasons, the CFAA Amendment should include an amendment to section 1030(g)[23] to maintain a civil cause of action even if the language set forth in subsection (c)(4)(A)(i)[24] is removed. The CFAA is very complicated,[25] highly nuanced, and laden with procedural hurdles that are interrelated and vital to effectively using the law.[26] Accordingly, those who draft proposed changes to the CFAA must thoroughly understand the law, the body of law surrounding it, and how it fits with other cyber-related laws on a grand scale. Without taking such a holistic approach, more mistakes are imminent.

II. Does the Amended Definition of "Exceeding Authorized Access" Find the Right Balance to Effectively Combat the Problems of Insider Misuse?

A. The Perceived Need for a New Definition of "Exceeding Authorized Access"

The primary structural change suggested in the CFAA Amendment is the revision of the CFAA's definition of "exceeds authorized access" to "mak[e] clear that it can be used to prosecute insiders who abuse their ability to access information to use it for their own purposes."[27] The purpose of this is to resolve what is commonly referred to as the circuit split:

---

21. Shawn Tuma, *Will Changes to the CFAA Deter Hackers?*, DarkMatters Superior Attack Intelligence Blog (Feb. 3, 2015), http://blog.norsecorp.com/2015/02/03/will-changes-to-the-cfaa-deter-hackers/.

22. *Id.*

23. 18 U.S.C. § 1030(g).

24. 18 U.S.C. § 1030(c)(4)(A)(i).

25. *See* Tuma, *"What Does CFAA Mean and Why Should I Care?"*, *supra* note 8, at 154 n.102.

26. *Id.*

27. CFAA Amendment, *supra* note 2.

> The Ninth Circuit's 2012 decision in United States v. Nosal created a circuit split regarding the interpretation of the phrase "exceeds authorized access" in the Computer Fraud and Abuse Act (CFAA). The Ninth Circuit (since joined by the Fourth Circuit) held that one "exceeds authorized access" to a computer by violating an *access* restriction (e.g., do not access File X), but not by violating a *use* restriction (e.g., do not use the computer for non-business purposes). This interpretation conflicts with the First, Fifth, Eighth, and Eleventh Circuits, which have held that use restrictions are within the scope of "exceeds authorized access."[28]

The circuit split focuses on the conflicting interpretations between the First,[29] Fifth,[30] Eleventh,[31] and Eighth[32] Circuits on the one hand, and the Ninth[33] and Fourth[34] Circuits on the other. But to be more accurate, there remain three distinct lines of interpretation.[35] The Trilogy of Access Theories include the Strict Access Theory, which describes the Ninth and Fourth Circuit approaches, the Intended-Use Theory, which describes the Fifth Circuit and its brethren, and the Agency Theory, which describes the still-binding precedent in the Seventh Circuit.[36]

B. The Courts Have Been Inconsistent in Distinguishing Between the Two Access Provisions

The CFAA Amendment is strictly focused on the definition of "exceeding authorized access," and many cases now focus on this prong as the point of contention.[37] However, the pertinent cases frequently avoid taking such a purist approach, and blur the lines between the "without authorization" and

28. Stuyvie Pyne, *The Computer Fraud & Abuse Act: Circuit Split & Efforts to Amend*, BERKLEY TECH. L.J. (Mar. 31, 2014), http://btlj.org/2014/03/31/the-computer-fraud-and-abuse-act-circuit-split-and-efforts-to-amend/.

29. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

30. United States v. John, 597 F.3d 263 (5th Cir. 2010).

31. United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

32. United States v. Teague, 646 F.3d 1119 (8th Cir. 2011).

33. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

34. WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

35. *See* Tuma, *"What Does CFAA Mean and Why Should I Care?"*, *supra* note 8, at 176.

36. Shawn E. Tuma, *Emp't Agreement Restrictions Determined Whether Emps. Exceed Authorized Access Under Computer Fraud & Abuse Act*, BUSINESS CYBER RISK LAW BLOG (Jan. 27, 2013), http://shawnetuma.com/2013/01/27/employment-agreement-restrictions-determined-whether-employees-exceeded-authorized-access-under-computer-fraud-and-abuse-act/.

37. CFAA Amendment, *supra* note 2.

"exceeding authorized access" prongs.[38] It would be preferable for courts and lawyers to carefully articulate which prong they are following.[39]

Moreover, while it is easy to become fixated on whether it is one or the other, the reality is that the legislation is being proposed is to solve a problem. That is, to establish a solution to the problem of insiders misusing their privileges. The problem needs no designation as to which prong it finds itself in, it simply needs a solution. If a solution to the problem is to be found, we must focus directly on the problem itself and work from there to find the solution. This is a better approach than trying to find solutions and then hoping to adapt them to the problem. In other words, we must first identify the objective and then work to find the appropriate solution. Accordingly, while the CFAA Amendment focuses on the "exceeding authorized access" language, this article will avoid being so limited and instead look at the cases and options that address the "without authorization" language as well.[40] Our objective is not to find the best definition for the "exceeding authorized access" prong or to find the best means of categorizing computer fraud cases as either unauthorized or excessive access cases. Rather, the proper objective is to find a means of controlling the problem of privileged users abusing their privileges by accessing computers and data which they then misuse.

III. Toward a Unified Theory of CFAA Access Jurisprudence

The framework of the Trilogy of Access Theories may be used to analyze the issue of insiders misusing their privileges to accomplish illicit purposes, but this article takes an alternative approach.[41] Just as the courts have struggled to fit the cases before them into the dichotomy of "without authorization" or "exceeding authorized access," so too have politicians, judges, lawyers, and commentators struggled to fit consistently the cases into one of the three main theories of access.[42] So too has the author of this article. Thus, going forward, instead of overcomplicating the analysis with false dichotomies, artificial definitions, or the like, we must simplify it by focusing on the problem.

The best way to address the problem is to stop analyzing cases in a framework that relies on a determination of which access theory those cases fall within, and instead, to simply analyze the primary CFAA access cases under a unified theory of CFAA Access Jurisprudence that categorizes the cases' factual scenarios and then considers if and how the respective jurisdic-

38. *See, e.g.*, *Miller*, 687 F.3d 199.

39. *See* Tuma, *"What Does CFAA Mean and Why Should I Care?"*, *supra* note 8, at 173-81.

40. Computer Fraud & Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030).

41. *See, e.g.*, Tuma, *Emp't Agreement Restrictions*, *supra* note 36.

42. *See, e.g.*, Pyne, *supra* note 28.

tions resolve the issue. This approach allows us to determine exactly where the problem lies. From there, we can apply the current CFAA's legal framework and contrast it against the proposed CFAA Amendment to determine whether the proposed amendment helps, hurts, or does not have much impact.

There are five primary fact patterns that describe most CFAA cases. It is initially helpful to envision with the mind's eye a continuum with points on each end and three points scattered throughout the middle. The following categories of case fact patterns represent the points on the continuum, with the first category being on the left end, the fifth on the right end, and the others in between:

(1) Privileged user without notice of owner's intended use misusing the computer or data during privileged access.[43]
(2) Privileged user with notice of owner's intended use, properly obtaining data during privileged access but later misusing data.[44]
(3) Privileged user with notice of owner's intended use, misusing the computer or data during privileged access.[45]
(4) Privileged user whose privileges are terminated before access of computer or data.[46]
(5) Non-privileged user access of computer or data.[47]

After analyzing the leading authorities in this context, the article will compare how they address the issues that the CFAA Amendment seeks to resolve, and determine whether the new definition will more effectively combat insider misuse.

A. The Proposed CFAA Amendment Language

The CFAA presently defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter. . . ."[48] The CFAA Amendment includes the following amended definition of "exceeds authorized access" with strikethrough text indicating deletion and italicized text indicating insertion of language in the current definition:

> (6) "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in ~~the~~ such computer—

43. *See, e.g.*, Int'l Airport Ctrs. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

44. *See, e.g.*, New Show Studios v. Needle, No. 2:14-cv-01250-CAS(MRWx), 2014 WL 2988271 (C.D. Cal. June 30, 2014).

45. *See, e.g.*, United States v. John, 597 F.3d 263 (5th Cir. 2010).

46. *See, e.g.*, United States v. Steele, No. 13-4567, 2014 WL 7331679 (4th Cir. 2014).

47. *See, e.g.*, United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

48. 18 U.S.C. § 1030(e)(6) (2008).

> (A) that the accesser is not entitled so to obtain or alter; or(B) for a purpose that the accesser knows is not authorized by the computer owner . . . .[49]

There are conflicting lines of authority that sometimes create difficulty in interpreting the statute. Likewise, there is a need to correct these conflicting lines of authority. The real question is, however, whether the CFAA Amendment is the answer.

B. The Five Categories of Cases on the Access Jurisprudence Continuum

1. Privileged User Without Notice of Owner's Intended Use Misusing the Computer or Data During Privileged Access

The starting point for analyzing the cases on the Access Jurisprudence Continuum is *International Airport Centers, LLC v. Citrin.*[50] This case involved an employee, Citrin, who was working in the real estate business and was lent a laptop from his employer "to record data that he collected in the course of his work in identifying potential acquisition targets."[51] Citrin decided to quit and go into business for himself, but before returning the laptop to his employer, "he deleted all the data in it—not only the data that he had collected but also data that would have revealed to [his employer] improper conduct in which he had engaged before he decided to quit."[52] Citrin did not simply "delete" the data in the normal course. Instead, he "loaded into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery."[53] His employer had no copies of what he deleted.[54]

Despite the fact that Citrin had been a privileged user at the time of his surreptitious activities, the Seventh Circuit did not restrict itself to analyzing the case as only one of "exceeding authorized access":

> Muddying the picture some, the Computer Fraud and Abuse Act distinguishes between "without authorization" and "exceeding authorized access," and, while making both punishable, defines the latter as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." That might seem the more apt description of what Citrin did.

49. CFAA Amendment, *supra* note 2.

50. Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006).

51. *Id.* at 419.

52. *Id.*

53. *Id.*

54. *Id.*

> The difference between "without authorization" and "exceeding authorized access" is paper thin, but not quite invisible. In *EF Cultural Travel BV v. Explorica, Inc.*, for example, the former employee of a travel agent, in violation of his confidentiality agreement with his former employer, used confidential information that he had obtained as an employee to create a program that enabled his new travel company to obtain information from his former employer's website that he could not have obtained as efficiently without the use of that confidential information. The website was open to the public, so he was authorized to use it, but he exceeded his authorization by using confidential information to obtain better access than other members of the public.[55]

The Seventh Circuit found this case to be different. Citrin terminated his agency relationship when he breached his duty of loyalty to his employer, "and with it his authority to access the laptop, because the only basis of his authority has been that relationship."[56] The court treated this "insider" case as an "outsider" or "without authorization" case under the CFAA.[57]

The *Citrin* approach is referred to as the Agency Theory. From the perspective of the computer owner, it is the most permissive of the three main theories of access, and it requires very little subversive behavior by a privileged user to find that he exceeded his authorized access.[58] Envision the Agency Theory as being the point on the far left end of the Trilogy Continuum. There is some question as to whether the Seventh Circuit would adhere to this approach now. The other circuit courts that have addressed this issue would not follow such a lax standard.

a. Will the CFAA Amendment Impact these Cases?

It is possible that under the proposed "exceeding authorized access" language, a court would find that Citrin was accessing the computer "for a purpose that [he] knows is not authorized by the computer owner,"[59] but it is far from certain. In the jurisdictions that have recognized privileged users exceeding authorized access violations, they have typically required a clear and unequivocal notice, setting forth the intended-use and prohibited uses for their access.[60] There would surely be litigation on this point.

---

55. *Id.* at 420 (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001)).

56. *Citrin*, 440 F.3d at 420–21.

57. *Id.*

58. *See id.*

59. *Id.* at 418.

60. *See* United States v. John, 597 F.3d 263 (5th Cir. 2010).

2. Privileged User with Specific Notice of Owner's Intended Use, Properly Obtaining Data During Privileged Access but Later Misusing Data

a. New Show Studios LLC v. Needle

While this scenario could manifest in many ways, there is a recent example in *New Show Studios LLC v. Needle*.[61] In *New Show Studios*, a former employee continued to use his former employer's information after his termination by having current employees access information and supply it to him. The court dismissed the CFAA claim because the plaintiff did not plead any access to a computer:

> To prevail on a CFAA claim, plaintiffs must establish, among other things, that defendants "intentionally accessed a computer." But the [first amended complaint (FAC)] is devoid of any allegation that the defendants accessed any computer. Instead, the FAC only alleges that Needle "gained access to confidential and sensitive information." Accessing plaintiffs' information, however, is not the same thing as accessing plaintiffs' computer systems, even if that information was at some point stored on those computers. The Ninth Circuit has specifically cautioned against reading the CFAA as an "expansive misappropriation statute." If plaintiffs wish to assert a claim under the CFAA, they must plainly allege that defendants' [sic] accessed their computer systems, and explain the basis for those allegations.[62]

As *New Show Studios* demonstrates, it is quite a challenge to find ways to use the CFAA, a law that has been defined as an "access violation," to protect data that was properly obtained and keep it from being misused at a later time.

b. Dice Corporation v. Bold Technologies

The Sixth Circuit highlighted the necessity for wrongful access in *Dice Corp. v. Bold Technologies*.[63] There, the parties were competing providers of alarm monitoring software that provided their software to companies in the alarm industry.[64] ESC Central was plaintiff's customer and had a database that stored large amounts of data for ESC's customers, including "names, addresses, contact information, billing information, and information regard-

61. New Show Studios v. Needle, No. 2:14-cv-01250-CAS(MRWx), 2014 WL 2988271 (C.D. Cal. June 30, 2014).

62. *Id.* at *6.

63. Dice Corp. v. Bold Tech., 556 F. App'x 378 (6th Cir. 2014).

64. *Id.* at 379.

ing the type and location of alarms."[65] ESC became dissatisfied with plaintiff and moved its business to defendant, Bold Technologies.[66]

To facilitate a seamless transition for ESC's customers, defendant wrote a program to extract ESC's data from plaintiff's software and convert it into a format that could be read by defendant's software.[67] Under normal operations, ESC could access plaintiff's database files of ESC's customer data and retrieve the data without circumventing any of plaintiff's security measures.[68] Also during this time period, one of plaintiff's employees went to work for defendant and assisted in the transfer of ESC's data from plaintiff to defendant. Plaintiff sued defendant for violating the Computer Fraud and Abuse Act. The plaintiff's claims were premised on the allegation that the employee accessed plaintiff's servers while working for defendant,[69] which the employee flatly denied.[70]

In deposition, plaintiff admitted that it had no evidence of when or how the employee allegedly hacked into its servers. Plaintiff stated:

> I don't know how Bold got our–got all of our intelligence. . . . It's not a question for me to answer, it's a question for you to answer. How did Bold get access to those files[?] . . . I don't know how Bold got the information to be able to do what they've done. I have no idea. All I know is that they have it. . . .[71]

The district court granted summary judgment for defendant because plaintiff admitted that it had no evidence; indeed, plaintiff had no idea of when, how, or specifically whether the former employee actually accessed its server after her employment terminated.[72] The employee offered a plausible explanation for how the information was obtained that did not involve her accessing plaintiff's server, which supported the defendant's motion and warranted summary judgment.

Plaintiff appealed to the Sixth Circuit, which affirmed the district court's grant of summary judgment on all claims.[73] The Sixth Circuit found the Computer Fraud and Abuse claim failed because the plaintiff failed to

65. *Id.*

66. *Id.* at 380.

67. *Id.*

68. *Id.*

69. *Dice Corp.*, 556 F. App'x at 381.

70. *Id.* at 388.

71. Dice Corp. v. Bold Tech., 913 F. Supp. 2d 389, 398–99 (N.D. Mich. 2012) (alterations and omissions in original).

72. *Id.* at 416.

73. *See Dice Corp.*, 556 F. App'x at 388.

show intentional access, which is required under the CFAA.[74] In this case, plaintiff claimed that the defendants wrongfully accessed its servers by performing a "Go To Assist Function" to access those servers.[75] The defendants, however, were unaware that by performing a "Go To Assist Function" they could access plaintiff's servers.[76] Accordingly, they could not have intentionally accessed the servers and there was no CFAA violation. The Sixth Circuit noted that "Even assuming this claim [was] fairly raised, it would still fail. Liability under the CFAA requires a showing of intentional access. Neither Narowski nor Condon was aware that performing a Go To Assist Function on ESC Central servers allowed access to Dice servers in Bay City, Michigan."[77]

i. Will the CFAA Amendment Impact these Cases?

The circuit courts have not addressed the specific fact pattern that is described above. It is included because it is likely to occur, and would not violate the CFAA Amendment.[78] In this scenario, a privileged user has been given authorization to access the owner's computer and data for specific purposes, and those purposes are clearly communicated to the privileged user.[79] The user then accesses the computer, obtains data that she uses for the intended purpose, and retains the data.[80] Her access to the computer and the data was proper, and for its intended use.[81] Subsequently, the basis for providing access—in this example, employment—is terminated. The person then goes to work for a competitor, discovers she still has the former employer's data and, for the first time, decides to use it (and does use it) for an improper purpose.[82] Would this be a violation of the proposed "exceeding authorized access" definition?

Under this scenario, it should not be a violation due to exceeding authorized access or access without authorization.[83] The proposed definition focuses on the accesser's intent—her state of mind—at the time of access, and it requires that the accesser "know" the purpose of access is not author-

74. *Id.*

75. *Id.* at 387.

76. *Id.* at 388.

77. *Id.* (internal citation omitted).

78. *See* CFAA Amendment, *supra* note 2.

79. *See Dice Corp.*, 556 F. App'x 378; *see also* New Show Studios v. Needle, No. 2:14-cv-01250-CAS(MRWx), 2014 WL 2988271 (C.D. Cal. June 30, 2014).

80. *See Dice Corp.*, 556 F. App'x 378.

81. *Id.*

82. *Id.*

83. *See* CFAA Amendment, *supra* note 2.

ized by the computer owner.[84] Under this definition, at the time of access, the acceser neither had an improper purpose nor knew of an improper purpose, which would not come into existence until some point in the future.[85] But the problem with attempting to draft CFAA language to cover this scenario is that it would require CFAA's prohibitions to continue to attach to the data long after the time of its access and its separation from the computer.[86]

There are now two focal points in this analysis: the device, and the data that is no longer associated with the device.[87] The CFAA has always focused primarily on wrongful access to computers (*i.e.*, the device).[88] Endeavoring to extend the CFAA to the realm of the data far beyond its separation from the computer is much more like trade secrets that focus on the data itself.[89] This means that at least under the current understanding of the CFAA, this is an issue that cannot be covered by the CFAA, or at least not by the CFAA alone.[90] This is problematic because, at least on a high level, this is one of the key issues of "insider misuse" that the CFAA Amendment is intended to address.[91]

3. Privileged User with Specific Notice of Owner's Intended Use, Misusing the Computer or Data During Privileged Access

This category of cases is closer to the middle on the Access Jurisprudence Continuum, and is the one that has received the most attention and stirred up most of the controversy over the circuit split.[92] There are two lines of legal authority within this category, those cases in which courts have found the accesses were wrongful in violation of the CFAA, and those in which they did not. The courts have not arrived at these holdings by adhering to a strict dichotomy of whether it was by exceeding authorized access or access without authorization, and neither will this article.[93] This is likely the category of cases to which the CFAA Amendment is primarily directed.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *See* CFAA Amendment, *supra* note 2.

90. *Id.*

91. *Id.*

92. *See, e.g.*, United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); *see also* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (citing Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000)).

93. *See John*, 597 F.3d at 271.

a. Cases Found to be Wrongful Access CFAA Violations

i. *United States v. John*

The leading case finding a wrongful access CFAA violation where a privileged user misused the data obtained from a computer even though the owner provided specific notice of the intended-use is *United States v. John*.[94] *John* involved a defendant that worked for Citigroup as an account manager who was authorized to access the company's computer system containing customer account information.[95] Citigroup's policies prohibited the misuse of company computers and information.[96] In violation of those policies, the defendant obtained customer account information, which she then provided to others who used the information to make fraudulent charges on the accounts.[97] At trial, the defendants were convicted for violating the CFAA by exceeding authorized access to a protected computer.[98] The Fifth Circuit upheld the conviction, holding that an owner of a computer (and the right of access) can establish policies limiting *the use* of information obtained by permitted access to a computer system and the data available on that system.[99] The violation of these policies exceeds authorized access under the CFAA.[100]

The *John* court applied the "exceeding authorized access" prong of CFAA access violations, not its earlier reasoning in *United States v. Phillips*,[101] which dealt with the "without authorization" prong.[102] In doing so, the court explained its "intended-use analysis" as follows: access to a computer, as well as the permissible use of the information available from the computer, can be defined by the owner's policies, and any access or use in violation of those policies exceeds authorized access.[103]

ii. *United States v. Rodriguez*

Soon after *John*, the Eleventh Circuit, in *United States v. Rodriguez*,[104] applied the same reasoning as that of *John* to find that the owner of access to a computer can define the limits of the privileges to access or use of the

94. *Id.*

95. *Id.*

96. *Id.* at 269.

97. *Id.*

98. *Id.* at 269–70.

99. *Id.* at 272–73.

100. *John*, 597 F.3d at 272–73.

101. United States v. Phillips, 477 F.3d 215 (5th Cir. 2007).

102. *John*, 597 F.3d at 271–72 (citing *Phillips*, 477 F.3d at 219).

103. *Id.* at 272–73.

104. United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

computer and stored data through its policies. As a result, any access or use of the computer or stored data exceeds authorized access.[105] *Rodriguez* involved a situation in which an employee of the United States Social Security Administration had improperly accessed personal information—that he was authorized to access for business purposes—in violation of the Administration's policy.[106] The Eleventh Circuit upheld his conviction, holding that "Rodriguez exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness reason."[107]

The court's rationale looked to the Administration's clear policy prohibiting such conduct; when Rodriguez violated the policy, he therefore exceeded his authorized access.[108] Essential in these cases finding wrongful access violations of the CFAA is the Administration's implementation of policies limiting the authorization of access to work computers for business reasons only, as well as the Administration's efforts to ensure that the employees were aware of such policies.[109] Then, when the privileged individuals use their access to the computers and data for non-business purposes, they exceed the intended use as defined by the policies; and therefore, exceed their authorized use in violation of the CFAA.[110]

iii. *United States v. Teague*

Following the reasoning of *John* and *Rodriguez*, in *United States v. Teague*, the Eighth Circuit upheld the conviction of Sandra Teague for exceeding authorized access in violation of the CFAA.[111] Teague was an employee of Vangent Corporation, Inc., a Department of Education contractor with privileged access to the National Student Loan Data Systems—a database containing borrowers' private information.[112] Teague was "one of nine privileged users who accessed the student loan records of now-President Barack Obama. Teague was indicted for and convicted of one count of exceeding authorized access to a computer.[113]

105. *See id.* at 1263 (citing *John*, 597 F.3d at 269–72).

106. *Id.* at 1260.

107. *Id.* at 1263.

108. *Id.*

109. *Id.*

110. *Rodriguez*, 628 F.3d at 1263.

111. United States v. Teague, 646 F.3d 1119, 1120 (8th Cir. 2011).

112. *Id.* at 1121.

113. *Id.*

iv. *United States v. Tolliver*

In *United States v. Tolliver*,[114] the Third Circuit issued an unpublished opinion in which it upheld the conviction of a bank employee under the Computer Fraud and Abuse Act for accessing information for a non-business purpose. This was in violation of the bank's prohibition against employees looking at customers' accounts and personal information without a business purpose.[115] The indictment charged Tolliver with accessing a computer in excess of authorization to obtain a financial record.[116] In upholding the conviction, the Third Circuit found that "there was sufficient evidence from which to infer that Tolliver intentionally accessed the customers' accounts and that she did not have a business purpose to do so. As such, the government established that Tolliver exceeded her authorized access." The court therefore affirmed the defendant's conviction under the CFAA.[117]

v. *CollegeSource v. AcademyOne*

On February 5, 2015, the Third Circuit Court of Appeals issued *CollegeSource v. AcademyOne*, an unpublished opinion that was consistent in its rationale with *Tolliver*.[118] In *College Source*, a dispute arose between two companies competing in the college credit-transfer information market.[119] CollegeSource sued Academy One, alleging that AcademyOne misappropriated the contents of its online computer database to gather information for use in its own database.[120]

Specifically, CollegeSource provides an online catalog of information that allows paying subscribers to search and inspect over 50,000 digital course catalogs and other school related information culled by CollegeSource from the offerings of colleges throughout the United States.[121] CollegeSource endeavored to keep its competitors from obtaining this information by using various methods, including a browsewrap notice[122] declaring "that distribu-

114. United States v. Tolliver, 451 F. App'x. 97 (3rd Cir. 2011).

115. *Id.* at 100.

116. *Id.*

117. *Id.* at 103–04.

118. CollegeSource, Inc. v. AcademyOne, Inc., No. 12–4167, 2015 WL 469041 (3d Cir. Feb. 5, 2015).

119. *Id.* at *1.

120. *Id.*

121. *Id.*

122. *See generally* Venkat Balasubramani, *What's a Browsewrap? The Ninth Circuit Sure Doesn't Know*-Nguyen v. Barnes & Noble, TECH. & MKTG. LAW BLOG (Aug. 9, 2014), http://blog.ericgoldman.org/archives/2014/08/whats-a-browsewrap-the-ninth-circuit-sure-doesnt-know-nguyen-v-barnes-noble.htm (explaining, and criticizing, the Ninth Circuit's definition of a broweswrap as an online agreement posted on the bottom of a webpage).

tion and noncommercial use are prohibited."[123] CollegeSource also used a clickwrap agreement[124] that stated, "'by signing in above, I agree to be bound by the terms of the . . . Subscription Agreement' . . . [which] state[d]: '[t]his Subscriber Agreement and Terms of Use govern your use of CollegeSource Online' . . . [and] commercial use of the data is prohibited."[125]

AcademyOne was a direct competitor to CollegeSource, offering a free online alternative to CollegeSource. AcademyOne sought, unsuccessfully, to purchase a license to CollegeSource's database. After being denied, AcademyOne hired a Chinese contractor (Beijing Zhongtian-Noah Sports Science Co., LTD.) to download the information from its original sources—the individual schools' websites.[126] Ultimately, it was discovered that AcademyOne's database contained catalogs that bore CollegeSource's copyright and disclaimer.[127] Thus, CollegeSource sued AcademyOne for violating the Computer Fraud and Abuse Act, among other statutory provisions.[128] The district court granted summary judgment on the CFAA claims, CollegeSource appealed, and the Third Circuit affirmed the district court's rulings.[129]

While both the district court and the Third Circuit ruled against finding liability on the CFAA claims, the language used in the Third Circuit's opinion is instructive as its analysis is similar to that employed in *Tolliver*. Specifically, the court looks to see if AcademyOne downloaded information in violation of the Subscription Agreement[130] or any other contractual or technical limitation;[131] *i.e.*, whether the user of the site exceeded the limitations imposed for accessing and using the information.

Based on these cases, a privileged user's own subjective change in motivation for accessing the computer or data is not enough, by itself, to terminate authorization. The same was true in the *Citrin* case of the Seventh

123. *AcademyOne*, 2015 WL 469041, at *1.

124. *See* Balasubramani, *supra* note 122.

125. *AcademyOne*, 2015 WL 469041, at *1.

126. *Id.*

127. *See id.* at *2.

128. *See id.*

129. *Id.* at *10.

130. *See id.* ("There is no evidence, however, that those employees downloaded catalogs for commercial use in violation of the Subscription Agreement. . . .").

131. *See AcademyOne*, 2015 WL 469041, at *10. ("These materials were available without precondition to any member of the general public who clicked the link on the subscribing school's website and was thereby directed to CS's servers. Thus again, A1 obtained the materials in question without breaching any . . . contractual term of use.").

Circuit.[132]However, nothing requires that the owner of authorization expressly notify the user that his access is terminated (as we will see with one of the categories discussed, *infra*). Rather, the owner can preemptively implement certain restrictions on access and use of information obtained by policies and agreements that are known to the user. And courts will consider any access unauthorized under the CFAA if the user violates those limitations by accessing information and using it for improper purposes or for any other reason that is not for its intended use.

b. Cases with No Wrongful Access CFAA Violations

The leading cases, which come from the Ninth Circuit, find there was not a wrongful access CFAA violation where a privileged user misused data obtained from a computer, even though the owner provided specific notice of the intended use. For example, in *LVRC Holdings LLC v. Brekka*,[133] the Ninth Circuit expressly rejected the Seventh Circuit's rationale in *Citrin* and held that a strict interpretation of the CFAA prohibits only the unauthorized access to a computer, rather than the corresponding unauthorized use of improperly obtained information.[134] According to *Brekka*, once an employee is authorized to access a company computer, authorization of his access continues even if his loyalties to his employer change and he begins doing another's bidding.[135] Regardless of an employee's subjective loyalties and intentions, or overt actions, the employer must expressly terminate his authorization.[136]

In April 2011, the Ninth Circuit briefly departed from this rationale, and distinguished *Brekka*, when a panel of the court decided *United States v. Nosal* (*Nosal I*).[137] The Ninth Circuit explained that when a computer owner has placed limitations on the privileges a user is given, and the user violates—or exceeds—those limitations, the user exceeds his authorized access.[138] This new rationale did not last long; nearly a year later, in April 2012, the Ninth Circuit reverted to its earlier position in *Brekka* when it decided the second *United States v. Nosal* (*Nosal II*).[139] In *Nosal II*, the court

132. *See* Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (citing RESTATEMENT (SECOND) OF AGENCY §§ 112, 387 (1958) ("Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.")).

133. 581 F.3d 1127, 1133 (9th Cir. 2009).

134. *See id.* at 1134–35.

135. *See id.* at 1133–34.

136. *See id.* at 1135.

137. *See* United States v. Nosal, 642 F.3d 781, 782 (9th Cir. 2011).

138. *Id.* at 787.

139. *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

held that "'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[140]

Soon thereafter, in July 2012, the Fourth Circuit followed the same line of reasoning as the Ninth Circuit when it decided *WEC Carolina Energy Solutions, LLC v. Miller*, essentially adopting the Ninth Circuit's rationale in *Nosal II*.[141] *WEC Carolina* did not add much to the substantive analysis on this issue, so *Nosal II* remains the standard. Envision these cases as falling near the middle but to the right of the Third, Fifth, Eighth, and Eleventh Circuits on the Trilogy Continuum.

c. *Will the CFAA Amendment Resolve the Confusion with These Cases?*

The purpose of the CFAA Amendment is to clearly establish a cause of action allowing for "[prosecution of] insiders who abuse their ability to access information to use it for their own purposes."[142] This is a broad definition that encompasses multiple different categories of cases. The CFAA Amendment is designed to eliminate confusion in this line of cases and establish some consistency in holding privileged users responsible for the misuse of information. Whether it will achieve these purposes, however, is not so clear.

The same issues regarding the timing of the intent that the court discussed in *Dice Corporation v. Bold Technologies* apply here. There are several other issues and questions that arise here as well. For example, it remains unclear what it means to "know" under the new Amendment language. As discussed above, both *John* and *Rodriguez* required that the owners establish clear designations of intended and prohibited use for the computers, as well as actual knowledge of those designations by the accessers. On the other hand, the CFAA Amendment only requires that the access be for a purpose that the accesser knows is not authorized to support a violation. This is a lower standard compared to the requirements of the Fifth and Eleventh Circuits. As a result, there are some questions as to whether those circuits will require the same level of knowledge as under the prior CFAA language, or whether they will start from scratch in applying the new text. Another question to consider is whether the new standard reaches down to the level of what *Citrin* found as sufficient to revoke authorization to access, such as a subjective change of loyalties.

Similarly, what does "is not authorized" mean under the new Amendment language? Does this mean that any use is prohibited unless it is specifically authorized? Or, does it mean that any use is authorized unless it is specifically identified as being not authorized? Many companies have poli-

140. *Id.* at 864 (emphasis in original).

141. *See* WEC Carolina Energy Sols., LLC v. Miller, 687 F.3d 199, 203, 207 (4th Cir. 2012).

142. CFAA Amendment, *supra* note 2.

cies that authorize the use of the computer system for "business purposes only" and prohibit use of the computer system for non-business purposes.[143] Will the law apply differently depending on whether a company has one, the other, or both of these statements in their Acceptable Use Policy?

Overall, the CFAA Amendment adds some guidance by making it clear that the CFAA, as amended, intends to prohibit misuse by insiders on a more granular level. However, this is the extent of the guidance. In reality, the Amendment raises more questions than answers, which means there will be considerable litigation over the new language. Finally, the CFAA will not become more certain and predictable, but rather will become just the opposite.

4. Privileged User Whose Privileges Are Terminated Before Access of Computer or Data

a. United States v. Steele

On December 24, 2014, the Fourth Circuit issued its opinion in *United States v. Steele*, which explains its view on and application of the CFAA's "exceeds authorized access" language.[144] Despite this explanation, the case only directly involved the court's application of the "without authorization" language to a former privileged user.[145]

The defendant, Robert Steele, was a former vice president of business development for Platinum Solutions, Inc.[146] Steele also served as the company's backup information technology systems administrator.[147] This responsibility provided Steele with the opportunity to access and monitor employee email accounts, including their passwords, and to set up a "backdoor" account into the company network.[148] Platinum's business was providing contract IT services to government defense agencies.[149] When Platinum was sold to SRA International, Inc., Steele subsequently resigned his employment and went to work for a competitor.[150] For nine months following his resignation, Steele continued to log in to SRA's network via the "backdoor" account to download documents and emails related to SRA's ongoing contract bids.[151]

143. *See* Tuma, *"What Does CFAA Mean and Why Should I Care?"*, *supra* note 8 (explaining that companies can restrict the employee's use of company computers and data).

144. United States v. Steele, No. 13-4567, 2014 WL 7331679 (4th Cir. 2014).

145. *Id.* at *1.

146. *Id.*

147. *Id.*

148. *See id.*

149. *Id.*

150. *Steele*, 2014 WL 7331679, at *1.

151. *Id.*

Steele continued to have access to the "backdoor" account as SRA had not changed Steele's password to this account.[152] An FBI investigation concluded that Steele accessed the SRA server nearly 80,000 times, which led to Steele's conviction on two misdemeanor and twelve felony counts under the CFAA for accessing the SRA server "without authorization."[153]

Steele appealed to the Fourth Circuit Court of appeals, arguing that his actions did not violate the CFAA "because SRA did not change his access password when he resigned, [and his] post-employment access, though 'ethically dubious' was not 'without authorization' as contemplated by the statute."[154] Steele relied on *WEC Carolina Energy Solutions LLC v. Miller* to support his argument.[155] In *Miller*, after analyzing the definition of "authorization" as used in the CFAA, the Fourth Circuit found that Miller accessed the information prior to his resignation and thus was not in violation of accessing "without authorization" under the CFAA.[156] In *Steele*, the Fourth Circuit upheld its definition of "authorization" developed in *Miller*, but distinguished the two cases based on the timing of the revocation of the access privilege occurred:

> Importantly, this split focuses on employees who are authorized to access their employer's computers but use the information they retrieve for an improper purpose. Steele's case is distinguishable for one obvious reason: he was not an employee of SRA at the time the indictment alleges he improperly accessed the company's server. . . . [T]he fact that Steele no longer worked for SRA when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed.[157]

Building on this reasoning, the court looked at the trial evidence and found that it provided ample support for the conviction:

> SRA took steps to revoke Steele's access to company information, including collecting Steele's company-issued laptop, denying him physical access to the company's offices, and generally terminating his main system access. And Steele himself recognized that his resignation effectively terminated any authority he had to access SRA's server, promising in his resignation letter that he would not attempt to access the system thereafter. Just because

152. *Id.*

153. *Id.*

154. *Id.* at *2.

155. *Id.*

156. *See* WEC Carolina Energy Sols., LLC v. Miller, 687 F.3d 199, 203, 207 (4th Cir. 2012).

157. *Steele*, 2014 WL 7331679, at *2 (citing LVRC Holdings v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009); RESTATEMENT (THIRD) OF AGENCY § 3.09 (2006)).

> SRA neglected to change a password on Steele's backdoor account does not mean SRA intended for Steele to have continued access to its information.[158]

What is intriguing about the Fourth Circuit's analysis in the *Steele* decision is its refusal to acknowledge the Fifth and Eleventh Circuit cases and their progeny. The *Steele* court began its discussion by describing the circuit split in an intriguing manner, particularly, the choice to reference the "broad view" in the circuit split.[159] Rather than providing a more accurate description of this broad view by including reference to the Fifth Circuit's *John* opinion or the Eleventh Circuit's *Rodriguez* opinion, the court instead comparted its preferred "narrower view," to the questionable *Citrin* opinion of the Seventh Circuit, saying:

> The broad view holds that when employees access computer information with the intent to harm their employer, their authorization to access that information terminates, and they are therefore acting "without authorization" under § 1030(a)(2). The narrower construction, adopted by *WEC Carolina*, holds that § 1030(a)(2) applies to employees who unlawfully *access* a protected computer, but not to the improper *use* of information lawfully accessed.[160]

It is curious that the Fourth Circuit relied on *Citrin* to contrast its preferred narrower view of the Ninth and Fourth Circuits. Importantly, the court did not even mention what has become the majority view, which is represented by at least four of its sister circuits.[161] Indeed, the court in *WEC Carolina* made no mention of this alternative view, the cases explaining it, or even its sister-circuits that follow that view. Even more curious is the fact that the court in *WEC Carolina* heavily relied on *Nosal II*, in which the Ninth Circuit at least acknowledged the existence of this line of authority, though it did not analyze its rationale.[162]

While *Steele* is a recent case, it clarifies the termination point of a user's authorized access: when a user is given access privileges to a computer by virtue of a relationship with the computer's owner. Under this theory, any authorization to access the computer ends when the relationship ends. Thus, the court would deem any post-relationship accesses, regardless of how accomplished, as being made "without authorization" and in violation of the CFAA.

---

158. *Id.*

159. *See id.*

160. *Id.* at *2 (internal citations omitted).

161. *See* Pyne, *supra* note 28 and accompanying text.

162. *See* LLC v. Miller, 687 F.3d 199, 203, 203 (4th Cir. 2012); United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012).

b. Craigslist Inc. v. 3Taps Inc.

The Northern District of California decided *Craigslist Inc. v. 3Taps Inc.* in August 2013, addressing insiders, privileged users, and those who abuse their privilege.[163] The case discussed how courts are using the tools they have before them to resolve problems in the context of the conflicting lines of cases. This case dealt with a privileged user who used the information available on a website in a manner that the granting authority disapproved.[164] The court found that, in this situation, the granting authority could properly terminate the specific user's right to access the website, even though the website was generally available to the public.[165] Furthermore, any subsequent access by the user was "without authorization" and would violate the CFAA.[166]

The facts of *Craigslist Inc. v. 3Taps Inc.*[167] are instructive. 3Taps operated an online service that aggregated and republished ads from Craigslist in real time, which Craigslist viewed as illegally scraping content.[168] Because Craigslist is public, 3Taps argued it had authorization to access the website.[169] The court found the argument persuasive.[170] But what Craigslist did next made this case significant.

After learning about 3Taps' activities, Craigslist provided written notice to 3Taps stating, "[t]his letter notifies you that you and your agents, employees, affiliates, and/or anyone acting on your behalf are no longer authorized to access, and are prohibited from accessing craigslist's website or services for any reason."[171] Then Craigslist used the technological measures available to it by configuring its website to block access from IP addresses associated with 3Taps.[172] 3Taps ignored the notice letter and easily circumvented these efforts by simply using different IP addresses and proxy servers to successfully conceal its identity, and continued to access the website.[173]

Craigslist ultimately discovered these acts and sued 3Taps for violating the CFAA. The primary issue was whether the CFAA applies when the owner of an otherwise publicly available website takes steps to restrict access

163. Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178 (N.D. Cal. 2013).

164. *See id.* at 1180.

165. *See id.* at 1184.

166. *Id.*

167. *See id.* at 1178–81.

168. *Id.* at 1180.

169. *Craigslist, Inc.*, 964 F. Sup. 2d at 1182 (citing Pulte Homes, Inc. v. Laborer's Int'l Union of N. America, 648 F.3d 295, 304 (6th Cir. 2011) (public presumptively authorized to access "unprotected website")).

170. *Id.*

171. *Id.* at 1180–81.

172. *Id.* at 1181.

173. *Id.*

by specific entities.[174] The court reasoned that Craigslist made its website publicly available initially and, therefore, authorized access to the world.[175] Craigslist sought to revoke that permission on a case-by-case basis through its cease-and-desist letter and IP blocking measures.[176] The issue narrowed to whether Craigslist had the authority to de-authorize access in this manner.[177]

The court found that "[']authorization['] turns on the decision of the [']authority['] that grants—or prohibits—access."[178] Craigslist, as owner of the website, rescinded that permission for 3Taps so further access by 3Taps was "without authorization."[179] The court looked to the Ninth Circuit's *Brekka*[180] holding as confirming "that computer owners have the power to revoke the authorization they grant."[181] In *Brekka*, "an employee logged into his work computer with valid credentials provided by his employer and emailed valuable documents from the employer's computer to the employee's personal e-mail address for use in his own competing business."[182] The *Brekka* Court reasoned that the plain language of the CFAA indicates that authorization depends on actions taken by the employer.[183] Therefore, a person uses a computer "without authorization" under [the CFAA] when the person has not received permission to use the computer for any purpose (such as a when a hacker accesses someone's computer without any permission) *or when the employer has rescinded permission to access the computer* and the defendant uses the computer anyway.[184]

3Taps's access was unauthorized even though Craigslist authorized the world to access the public information on the website because "just as *Brekka* instructed that an 'authority' can do, it rescinded that permission for 3Taps. Further access by 3Taps after that rescission was 'without authorization.'"[185]

---

174. *See id.*

175. *Craigslist, Inc.*, 964 F. Supp. 2d at 1182.

176. *Id.*

177. *Id.*

178. *Id.* at 1184.

179. *Id.* at 1183.

180. LVRC Holdings v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009).

181. *Craigslist Inc.*, 964 F. Supp. 2d at 1183 (citing *Brekka*, 581 F.3d at 1129–30, 1134).

182. *Id.*

183. *See id.* (citing *Brekka*, 581 F.3d 1127).

184. *Id.* (emphasis added).

185. *Id.* at 1184.

c. Facebook, Inc. v. Grunin

The Northern District of California decided a similar case on January 8, 2015. In *Facebook, Inc. v. Grunin*, Grunin created fraudulent accounts on Facebook, which is free and open to virtually all.[186] With these fraudulent accounts, he set up a scheme to bilk Facebook out of a substantial amount of advertising revenue.[187] Similar to *Craigslist*, Facebook sent cease and desist letters terminating Grunin's authorization to access the site and implemented technical measures to block his access.[188] Grunin continued his scheme and ultimately generated advertising fees in excess of $340,000.[189] Facebook sued, and the court, relying in part on *Brekka* and *Craigslist*, found his accesses were "without authorization," and in violation of the CFAA.[190] According to *Craigslist*, the CFAA allows the owner of the subject computer to terminate access to that computer if it provides clear and unambiguous notice.[191] Facebook followed that procedure exactly, but Grunin ignored the notice. He deliberately violated Facebook's requests by continuing to access the website, essentially demanding Facebook pay a ransom to stop his scheme.

The courts have not yet distinguished between accesses that are "without authorization" and those "exceeding authorized access." In many cases, the boundaries between the two not only blur, but overlap.[192] However, *Craigslist* narrowed the playing field in terms of how to deal with disloyal insiders. When there is a known, disloyal insider, the owner of access can provide notice terminating the authorization and limiting the former privileged user from continuing to access or use the computer or information. If the user circumvents those limits, all subsequent accesses will be "without authorization" and therefore will violate the CFAA.

On the heels of *Craigslist*, two issues remain: (1) how to deal with the unknown disloyal insider; and (2) how to preemptively deal with the privileged user's misuse of computer information before the granting authority is able to terminate authorization.

d. NetApp, Inc. v. Nimble Storage, Inc.

A recent California district court case demonstrates similar factual circumstances and outcomes to *Steele*. In *NetApp, Inc. v. Nimble Storage, Inc.*,

186. Facebook, Inc. v. Grunin, No. C 14-02323 WHA, 2015 WL 124781, at *4 (N.D. Cal. Jan. 8, 2015).

187. *See id.*

188. *Id.*

189. *Id.*

190. *See id.* at *4–5.

191. *See* Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178 (N.D. Cal. 2013).

192. *See* Tuma, *"What Does CFAA Mean and Why Should I Care?"*, *supra* note 8, at 174–75.

the court rejected the argument that technological barriers must exist to establish lack of authorization.[193] The court pointed out that "cases interpreting *Brekka* and *Nosal* indicate that a nontechnological barrier can revoke authorization."[194] In *NetApp*, one defendant, a former employee of Nimble with access to NetApp's computer system, continued to use his login credentials to access NetApp's system after their relationship ended.[195] NetApp sued the employee under the CFAA, claiming he was accessing its protected computer system without authorization.[196] The employee did not deny that he accessed information without permission.[197] Instead, he argued his access did not violate the CFAA because NetApp had not disabled his login credentials.[198] According to the employee, the CFAA required NetApp to establish technological barriers to the former employee's access to demonstrate a lack of authorization.[199]Without an actual circumvention of such barriers, the defendant argued, there could be no CFAA violation.[200] NetApp countered that the existence or circumvention of technological barriers is not necessary to establish a CFAA violation.[201] The court agreed, finding that the weight of current authority supportedNetApp's interpretation.[202]

i. *NetApp*'s Homeowner/Houseguest Analogy Applied

In reaching this decision, the *NetApp* court examined numerous cases that the employee argued supported his position, but ultimately found that they failed to justify his arguments.[203] Following its analysis, the court entertained a helpful analogy:

> NetApp analogizes this case to a conventional property crime, arguing that "[u]nder Reynolds' theory, a thief has license to burglarize a house because a window is left open." However, a closer analogy would be a situation where a houseguest receives a key, [then is] told he is no longer welcome but keeps the key, and the homeowner neglects to change the lock. Reynolds's arguments suggest that if the former houseguest continues to reenter the

193. *See* NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK (HRL), 2014 WL 1903639, at *10 (N.D. Cal. May 12, 2014).

194. *Id.*

195. *Id.* at *1.

196. *Id.* at *2.

197. *See id.* at *8.

198. *Id.*

199. *NetApp, Inc.*, 2014 WL 1903639, at *8.

200. *Id.*

201. *Id.*

202. *Id.* at *9.

203. *See id.* at *10–11.

> house, the houseguest would not be acting "without authorization" or "exceed[ing] authorized access," even though he knows he may not return. Current CFAA doctrine does not allow this result. Accordingly, Reynolds's arguments do not warrant dismissal of any of NetApp's CFAA claims on this basis.[204]

To put the case into perspective, the analogy need only be taken one step further. Instead of the houseguest taking his key and leaving after being told he is no longer welcome, he surreptitiously changes the locks, forces the homeowners out, and does not allow them to reenter their own home. He then claims no CFAA violation occurs because the homeowners did not use barriers to keep him out—after he had already locked them out and was in complete control!

e. Weingand v. Harland Fin. Solutions, Inc.

In *NetApp, Inc.*, the court heavily relied on its decision in *Weingand v. Harland Financial Solutions, Inc.*, an instructive and factually similar case.[205] In *Weingand*, an employer granted its former employee post-termination permission to retrieve his "personal files" from the company's computer.[206] In its CFAA counter-claim, the company alleged that the former employee had "accessed, without authorization, over 2,700 business files."[207] However, the employee argued that his access was not without authorization because the company did not establish technical barriers to keep him from accessing the files.[208] The court disagreed, stating that,"Ninth Circuit authority (un-altered by *Nosal*) indicates that if a former employee accesses information without permission, even if his prior log-in information is still operative as a technical matter, such access would violate the CFAA."[209] The court explained:

> Although Plaintiff's counsel contended at oral argument that Plaintiff's level of verbal (or non-technical) authorization was irrelevant because the only "authorization" to which the statute speaks is "code" authorization (*i.e.*, whether someone is literally blocked from certain files by some security measure such as a password), Plaintiff offers no authority to support such a narrow interpretation. It is true that *Nosal* uses the phrase "physical access" to describe the expansive interpretation of the CFAA the

204. *Id.* at *11 (internal citations omitted).

205. *See NetApp, Inc.*, 2014 WL 1903639, at *10 (citing Weingand v. Harland Fin. Solutions, Inc., No. C-11-3109 EMC, 2012 WL 2327660, at *2, *7–9 (N.D. Cal. June 19, 2012)).

206. *Weingand*, 2012 WL 2327660, at *2.

207. *Id.* at *1.

208. *Id.* at *3.

209. *Id.* (citing LVRC Holdings v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009)).

> government proposed (and the court rejected). However, the previous sentence of the opinion makes clear that the court was concerned only with the distinction between access and use, not with any distinction between types of authorization pertaining to access.[210]

f. Will the CFAA Amendment Impact these Cases?

The CFAA Amendments were designed to focus on the misuse of access and data by privileged users, not users whose privileges were either terminated or never existed. Generally, courts find that non-privileged users have accessed a computer "without authorization," but the amendments focus on users who "exceed[ ] [their] authorized access."

Case law demonstrates that owners who are aware of misuse may terminate authorization with clear notice, rendering any subsequent access a violation of the CFAA. This is true even in jurisdictions where courts are reluctant to find authorization abuse or the misuse of information by a privileged user. Additionally, notice provides computer owners with a remedy for prior misuse of computers or data by privileged users by terminating the authorization needed for future misuse. However, notice does not provide a tool for owners to use proactively. Thus, the issue of preventing privileged users from accessing and misusing information remains unresolved.

5. Non-Privileged User Access of Computer or Data

This describes the conduct that most people think of when they hear the word "hacking"—someone who does not have any rights to access a computer is accessing it anyway. This leads back to the beginning of CFAA jurisprudence and the very first conviction under the CFAA in *United States v. Morris*.[211] Robert Morris was a "student in Cornell University's computer science Ph.D. program" who had "significant computer experience and expertise."[212] Morris, the original "security researcher," talked with classmates about security vulnerabilities and "began work on a computer program, later known as the INTERNET 'worm' or 'virus,'" to test his theories.[213] Eventu-

210. *Id.* (citing United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012)) (internal citation omitted).

211. *See* United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991); Joseph P. Daly, *The Computer Fraud & Abuse Act—A New Perspective: Let the Punishment Fit the Damage*, 12 J. MARSHALL J. COMPUTER & INFO. L. 445, 445 (1993) ("In *United States v. Morris*, the United States Court of Appeals for the Second Circuit heard the first criminal prosecution of a computer virus crime under the Computer Fraud and Abuse Act of 1986 . . . .").

212. *Morris*, 928 F.2d at 505.

213. *Id.* (explaining that Morris developed the program "to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that [he] had discovered.").

ally, Morris released his complex and stealth program "from a computer at the Massachusetts Institute of Technology . . . to disguise the fact that it came from [him] at Cornell."[214] The worm spread much faster "than he had anticipated" and "crashed" computers "around the country," "including [those at] leading universities, military sites, and medical research facilities."[215] The cost of Morris' security research project "at each installation ranged from $200 to more than $53,000."[216] The Second Circuit upheld Morris' conviction for accessing the various computers "without authorization."[217]

Since *Morris*, those prosecuted under the CFAA engaged in typical "hacking," like the "Anonymous" hackers,[218] the individuals who stole private information from other people's computers,[219] and foreign state sponsored hackers who attacked American companies.[220] The CFAA Amendment was not intended to impact and should not impact this category of cases.

IV. If This Is Not It, Then Where Do We Find the Golden Mean?

When stripping away the awkward structural framework into which the CFAA cases have been forced, as well the artificial labels that have been applied to those cases, one can see where the real root of the problem lies and where the focal point for the legislative fix—as well as the judicial fix—resides. The courts are forcing the CFAA cases into an awkward structural framework. When this framework is stripped away, the root of the problem becomes apparent. This is where the focal point for a legislative and judicial fix lies. How do we prevent privileged users from using their authorization to (1) misuse the computers or data during authorized use, or (2) misuse data

214. *Id.* at 505–06.

215. *Id.* at 506.

216. *Id.*

217. *Id.* at 505.

218. *See Jeremy Hammond Sentenced To 10 Years In Prison*, HuffingtonPost.com (Nov. 15, 2013, 2:37 PM), http://www.huffingtonpost.com/2013/11/15/jeremy-hammond-sentenced_n_4280738.html (reporting that Jeremy Hammond stole "files as part of the online hacking collective Anonymous.").

219. *See* Shawn E. Tuma, *Hunter Moore or Aaron Swartz: Do we hate the CFAA? Do we love the CFAA? Do we even have a clue?*, Business Cyber Risk Law (Jan. 24, 2014), http://shawnetuma.com/2014/01/24/what-do-we-want-do-we-hate-the-cfaa-do-we-love-the-cfaa-do-we-even-have-a-clue/ (discussing four individuals who were prosecuted under the CFAA).

220. *See* Press Release, U.S. Dep't of Justice Office of Pub. Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor ("The indictment alleges that the defendants conspired to hack into American entities . . . .").

obtained during an authorized use, after the time of the authorized access? This is the heart of the problem. This is the objective that was set forth by the President during his State of the Union address, in which he made his case for the CFAA Amendment.[221] Despite the President's admirable aspiration and efforts, unfortunately, it is unlikely that the CFAA Amendment will accomplish this objective.

The problem is that the CFAA is inherently designed to solve problems dealing with wrongful access of computers and data.[222] The courts have applied it, in a very thoughtful manner, to prohibit the wrongful use of computers or data during times of access. The current problem is that the point on the Access Continuum, where the problem lies, is post-access use of data. This necessarily requires legislation for judicial application of the rules to protecting the data and not the devices. While this could be done with the CFAA, in theory, it also intrudes upon trade secret law in many ways.[223] So perhaps, if there is a comprehensive solution, it will come through laying on the table both the proposed CFAA and the federal trade secret law.[224] Legislatures could meld them together into a seamless tool that is focused on solving the problems, and not trying to fit them in to an artificial category. This requires focusing first on the problem to be solved, not focusing on the tools to solve the problem that still lacks an accurate definition.

This leads to multiple conclusions. First, assuming the CFAA Amendment was not intended to negate the civil cause of action, Congress needs to correct the language to ensure there is no question as to its validity.[225] If it was intended to negate the civil cause of action, then that is a disastrous idea that must be stopped. Second, while the CFAA Amendment may theoretically help resolve some of the confusion about the application of the law to certain insider misuse situations, it would not resolve the primary problem of insider misuse/post-use of data.[226] Further, this causes more confusion and litigation, which is counterproductive as it leads to less predictability in the application of the law. Third, by rewriting the definition of "exceeding authorized access," we lose the ample body of jurisprudence interpreting the statute.[227]

What all of this shows is that ultimately, the CFAA Amendment is not a well-planned, comprehensive, and refined solution. But it is still valuable. The President offered many great concepts, and demonstrated a willingness

221. *See* CFAA Amendment, *supra* note 2.

222. *See* 18 U.S.C. § 1030 (2008).

223. *See* New Show Studios v. Needle, No. 2:14-cv-01250-CAS(MRWx), 2014 WL 2988271, at *1 (C.D. Cal. June 30, 2014).

224. *See* Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014).

225. *See* CFAA Amendment, *supra* note 2.

226. *See id.*

227. *See id.*

to attack this issue. Additionally, the President gave legislators more material to work with in trying to create an acceptable solution that will meet the stated objectives, or help to realize that the law cannot do so with this statute alone.

Have we found Aristotle's Golden Mean in terms of finding the proper balance for applying the Computer Fraud and Abuse Act to misuse by privileged users? Probably not. But the search continues and we have made, and continue to make, progress. We are narrowing the zone where it likely lies but we have not found the solution to the problem.

Case Notes